

ASSIGNMENT 5

Textbook Assignment: "AIS Security (continued)," chapter 4, pages 4-26 through 4-40; "General Security," chapter 5, pages 5-1 through 5-13.

- 5-1. The AIS technical manager can develop measures to use in case of emergency by reviewing operations and records with which of the following personnel?
1. Production control clerk
 2. Response team members
 3. Shift leaders
 4. Users
- 5-2. All personnel should be instructed to take which of the following security measures if an evacuation of work areas is ordered?
1. Secure classified material in desks or file cabinets
 2. Turn equipment and room lights off
 3. Close the doors as areas are evacuated but leave the doors unlocked
 4. Power up the air-conditioning equipment
- 5-3. To ensure that all safety requirements of the AIS facility are satisfied, the AIS technical manager and the operations division officer should review the protective plans with what frequency?
1. Monthly
 2. Quarterly
 3. Semiannually
 4. Annually
- 5-4. Backup operations may take place onsite under which of the following conditions?
1. A partial loss of capability
 2. Major damage only
 3. Major destruction only
 4. Major damage and destruction
- 5-5. For the purpose of making backup resources available, which of the following tasks can be set aside?
1. Short-term planning
 2. Program development
 3. Weekly processing
 4. Backup processing
- 5-6. When backup alternatives are considered, which of the following substitute procedures may be implemented during an emergency?
1. A hard disk input could be used for a failed telephone input
 2. Online processing could be substituted for batch processing
 3. Print tapes could be carried to a backup facility for offline printing
 4. Both 2 and 3 above

5-7. To evaluate alternate backup modes and offsite facilities, you should consider all but which of the following factors?

1. AIS hardware usage
2. Maintenance personnel for your AIS building
3. Overtime cost factor for civil service personnel
4. Transportation of personnel with needed supplies and materials

5-8. When developing the optimum backup plan, it is wise to form several backup plans, one of which has which of the following characteristics?

1. Extends beyond the cause of delay
2. Includes each minor partial failure
3. Lasts at least half the time required to reconstruct the facility
4. Includes one or more operating periods between minimum duration and worst case

5-9. Each COOP backup plan should cover a total of how many basic areas?

1. Five
2. Six
3. Three
4. Four

- A. Administrative information
 - B. Computer system specifications
 - C. Performance specifications
 - D. User instructions

Figure 5A

IN ANSWERING QUESTIONS 5-10 THROUGH 5-12, SELECT FROM FIGURE 5A THE AREA OF THE COOP BACKUP PLAN DESCRIBED.

5-10. The specific ways in which performance of each task departs from normal is stated.

1. A
2. B
3. C
4. D

5-11. Input in different forms may be required.

1. A
2. B
3. C
4. D

5-12. The location of the system is given.

1. A
2. B
3. C
4. D

5-13. The process of recovery will be carried out more effectively and economically if handled by which of the following personnel?

1. The users only
2. The AIS staff only
3. The users and AIS staff
4. Personnel other than the AIS staff

- 5-14. Before recovery from total destruction is achieved, all but which of the following tasks must be completed?
1. Locating floor space for the AIS facility without regard for live load capacity
 2. Verifying all needed hardware, equipment, and materials
 3. Performing facility modifications
 4. Procuring hardware
- 5-15. For COOP testing, a team should be assembled to perform all except which of the following tasks?
1. Prepare a scenario for the test
 2. Control and observe the test
 3. Evaluate the test results
 4. Provide training
- 5-16. Which of the following is a standard for an AIS facility inspection?
1. It should be dependent and subjective
 2. It should examine the information system and its use
 3. It should ignore adequacy controls
 4. It should be the first element in a physical security program
- 5-17. The characteristic of an inspection being independent and objective implies that the inspection has which of the following relationships to management?
1. Replaces normal management inspections
 2. Is a part of normal management visibility
 3. Complements normal management inspections
 4. Is a substitute for the management reporting, system
- 5-18. An inspection can be expected to accomplish which of the following tasks?
1. Evaluate security controls for the AIS facility
 2. Provide users an opportunity to maintain the AIS security program
 3. Provide the impetus to keep workers and management complacent
 4. Uncover adequate operational areas
- 5-19. In determining the frequency of internal inspections, the AIS technical manager should consider which of the following factors?
1. Operation workload
 2. The rate of change of the AIS
 3. The SOPS of the AIS staff
 4. The results of the last inspection only

- 5-20. What is the role of the inspection team?
1. To develop security controls
 2. To evaluate established controls
 3. To enforce control procedures
 4. To develop security procedures
- 5-21. Which of the following characteristics of the inspection board members will NOT affect the success of the inspection?
1. Ability
 2. Objectivity
 3. Probing nature
 4. Punctuality
- 5-22. Which of the following is NOT an important characteristic for the inspection board members?
1. Ability to enforce controls
 2. Attention to detail
 3. Inquisitiveness
 4. Probing nature
- 5-23. Which of the following types of expertise is helpful for a member of the inspection team?
1. Operations experience only
 2. Security experience only
 3. Security experience and programming knowledge
 4. Operations experience and programming knowledge
- 5-24. The group of people who have the most to gain from an effective inspection are the
1. members of the inspection team
 2. members of the security force
 3. programmers in the facility
 4. users of the facility
- 5-25. Which of the following is a characteristic of a comprehensive inspection plan?
1. It is action-oriented
 2. It lists actions to be bypassed
 3. It is tailored for universal installation
 4. It allows freedom in the report design
- 5-26. In developing a comprehensive inspection plan, what is the third step?
1. Review the risk analysis plan
 2. Examine the security policy and extract pertinent objectives
 3. Examine the AIS facility organization chart and job descriptions
 4. Review documents to determine the specified security operating procedures

- 5-27. When formulating the inspection program, which of the following areas is the most important to consider?
1. The most recent security breach without regard for security priorities
 2. The activities that produce minimum results with the most effort
 3. The critical issues with regard to security
 4. The measures that are tested most frequently in day-to-day operations
- 5-28. It is considered advantageous to test fire detection sensors under surprise conditions for which of the following reasons?
1. To test the response to alarms
 2. To test the reaction of the fire party
 3. To test the effectiveness of evacuation plans
 4. Each of the above
- 5-29. Why should the review of previous inspection reports be part of the process of developing an inspection plan?
1. To show trends
 2. To identify weaknesses that should have been corrected
 3. To identify strengths that were identified
 4. To identify previous team members
- 5-30. With what frequency should a scheduled inspection take place?
1. Monthly
 2. Quarterly
 3. Semiannually
 4. Annually
- 5-31. A surprise inspection should be approved by which of the following personnel?
1. The facility security officer
 2. The AIS technical manager
 3. The commanding officer of the command in charge of the AIS facility
 4. The commanding officer of the user command
- 5-32. In conducting a scheduled inspection, which of the following is normally the first step?
1. Interviewing the AIS personnel
 2. Scrutinizing the AIS facility records
 3. Inventorying the AIS hardware capabilities of the facility
 4. Testing the AIS facility access control procedures
- 5-33. Most security inspections include testing which of the following activities at AIS facilities?
1. Fire-fighting procedures
 2. Facility evacuation
 3. System backup
 4. Personnel placement procedures
- 5-34. What is the preferred frequency at which the inspection team should convene to review progress and compare notes?
1. At the end of each day's activity
 2. At the end of each week's activities
 3. Every 2 weeks
 4. Every 3 weeks

- 5-35. After the completion of the inspection, when should the written report be prepared?
1. When requested by the supervisor of the AIS facility being inspected
 2. When requested by the commanding officer of the AIS facility being inspected
 3. Immediately after the inspection, while the impressions are still fresh
 4. After an extended period of time to allow the inspection team members to reflect on the inspection process
- 5-36. Who is responsible for implementing the recommendations received from the inspection?
1. The AIS technical manager
 2. The security officer
 3. The commanding officer
 4. The TYCOM
- 5-37. The best approach in assigning responsibilities for corrective action is to summarize each major deficiency on a control sheet outlining which of the following areas?
1. An executive summary
 2. The action taken or required
 3. The date the deficiency was discovered
 4. The reporting official
- 5-38. For any control item that is still open, it is recommended that reports be turned in to upper management with what frequency?
1. Weekly
 2. Monthly
 3. Quarterly
 4. Semiannually
- 5-39. Which of the following instructions provides guidelines for implementing security safeguards required to implement the Privacy Act of 1974?
1. SECNAVINST 5211.5
 2. SECNAVINST 5239.2
 3. OPNAVINST 5510.1
 4. OPNAVINST 5239.1
- 5-40. Which of the following subsections of the Privacy Act (title 5, section 552a) requires the use of safeguards to ensure the confidentiality and security of records?
1. Subsection (b)
 2. Subsection (c)
 3. Subsection (e) (5)
 4. Subsection (e) (10)

- 5-41. A personal data security risk assessment benefits a command in all but which of the following ways?
1. It saves money that might have been wasted on safeguards that do not significantly lower the overall data risks
 2. It ensures that additional security safeguards help to counter all the serious personal data security risks
 3. It provides a basis for deciding whether additional security safeguards are needed for personal data
 4. It considers only the risks to personal data
- 5-42 . Which of the following participants should NOT be included on the risk assessment team?
1. A representative of the operating facility
 2. An individual responsible for security
 3. A system programmer
 4. A systems analyst
- 5-43. Data may be misrouted, mislabeled, or it may contain unexpected personal information as a result of which of the following data security risks?
1. Input errors
 2. Program errors
 3. Improper data dissemination
 4. Mistaken processing of data
- 5-44. When security measures to adequately control system access to personal data are developed, they should include protection from all except which of the following risks?
1. Dial-in access
 2. Open system access
 3. Physical destruction of the AIS
 4. Unprotected files and theft of data
- 5-45. Commands designing large computer networks should consider which of the following risks early in the planning stages?
1. Eavesdropping only
 2. Misidentified access and eavesdropping only
 3. Operating system flaws and subverting programs only
 4. Misidentified access, eavesdropping, operating systems flaws, subverting programs, and spoofing
- 5-46. Information management practices include all but which of the following activities?
1. Data collection, validation, and transformation
 2. Information processing or handling
 3. Information control, display, and presentation
 4. Managerial determination of the need and use of the information

- 5-47. Which of the following practices is/are suggested for the handling of personal data?
1. Label recording media that contain data of local personnel only
 2. Carefully control products of intermediate processing steps
 3. Maintain an online, up-to-date hardcopy authorization list of all individuals who have access to any data
 4. Both 2 and 3 above
- 5-48. Which of the following practices is/are suggested for the maintenance of personal records?
1. Establish procedures for maintaining correct, current accounting of all new personal data brought into the computer facility
 2. Maintain logbooks for terminals that are used to access any data by system users
 3. Both 1 and 2 above
 4. Log each transfer of storage media containing data to the computer facility
- 5-49. For a broader knowledge of personal identification and identification techniques, you should refer to which of the FIPS publications?
1. FIPS PUB 31
 2. FIPS PUB 48
 3. FIPS PUB 79
 4. FIPS PUB 114
- 5-50. Which of the following pieces of equipment might be considered a TEMPEST hazard?
1. Personal computer
 2. Electric typewriter
 3. Both 1 and 2 above
 4. A copying machine
- 5-51. The vulnerability of a ship or aircraft can be determined by which of the following means?
1. A TEMPEST survey
 2. A TEMPEST vulnerability assessment
 3. A TEMPEST investigation
 4. An emission control test
- 5-52. What is the purpose of EMCON?
1. To intercept and rebroadcast signals to confuse hostile forces
 2. To prevent hostile forces from detecting, identifying, and locating friendly forces
 3. To minimize the amount of transmission time on live circuits
 4. Both 2 and 3 above
- 5-53. What is the designation of security spaces requiring access control?
1. Controlled area
 2. Exclusion area
 3. Restricted area
 4. Limited area
- 5-54. Which of the following information should appear in a visitors log for a communications center?
1. Visitor's printed name and signature
 2. Purpose of visit and the escort's name
 3. Date and time of visit
 4. Each of the above

5-55. The combination to a classified material container must be changed at what maximum interval?

1. Monthly
2. Every 6 months
3. Every 12 months
4. Every 24 months

5-56. Which of the following statements concerning the security classification of a safe combination is correct?

1. All combinations are classified Secret regardless of the classification of contents stored within
2. All combinations are classified Confidential regardless of the classification of contents stored within
3. All combinations are handled as official information
4. Combinations are assigned a security classification equal to the highest category of classified material stored

5-57. An individual who is responsible for safeguarding and accounting for classified material is known by what term?

1. Custodian
2. User
3. Keeper
4. Guardian

5-58. Which of the following conditions for protecting classified material after working hours is NOT in accordance with security instructions?

1. Classified documents are in locked authorized containers
2. Classified notes, carbon paper, typewriter ribbons, and rough drafts have been destroyed or are in locked authorized containers
3. The contents of wastebaskets containing classified material were not burned, but are in locked authorized containers
4. Burn bags, ready for burning the next day, are securely stapled, numbered, and neatly lined up along the bulkhead

5-59. What is the minimum number of times the dial of a security container must be rotated in the same direction to ensure it is locked?

1. Five
2. Two
3. Three
4. Four

- 5-60. During routine destruction of classified material, what is the ultimate goal of the destruction?
1. To clear files of old material so there is more room for new material
 2. To make reconstruction of the material impossible
 3. To prevent unauthorized reproduction
 4. To destroy the material as quickly as possible
- 5-61. What is the most efficient means of destroying classified material?
1. Burning
 2. Shredding
 3. Jettisoning
 4. Pulping
- 5-62. Persons witnessing destruction of classified material must have a security clearance of at least what level?
1. Confidential
 2. Secret
 3. Top Secret
 4. The level of the material being destroyed
- 5-63. When is a record of destruction required for Secret messages?
1. If only one person performs destruction
 2. If the messages have special markings
 3. If the messages have to be jettisoned
 4. During routine destruction
- 5-64. Records of destruction of classified material must be maintained for what minimum length of time?
1. 1 yr
 2. 2 yr
 3. 6 mo
 4. 18 mo
- 5-65. How are burn bags accounted for prior to burning?
1. Bags are placed in a secure place and inventoried daily
 2. Each bag must be serially numbered and a record kept of all subsequent handling until destroyed
 3. Each office is responsible for its burn bag until the day of destruction
 4. On the day of destruction, each bag is serially numbered
- 5-66. What is the maximum allowable size of material shredded by a crosscut shredding machine?
1. 1/32 inch wide by 1 inch long
 2. 1/32 inch wide by 1/2 inch long
 3. 3/64 inch wide by 1/2 inch long
 4. 3/64 inch wide by 1 inch long
- 5-67. If classified material must be jettisoned during emergency destruction, what should be the minimum depth of the water?
1. 500 fathoms
 2. 700 fathoms
 3. 1,000 fathoms
 4. 5,000 fathoms

5-68. Which of the following areas must be covered in a command's emergency action plan?

1. Enemy actions
2. Civil disturbances
3. Natural disasters
4. Each of the above

5-69. When a command implements its emergency plan, the priority of destruction should be based on what factor?

1. The speed at which the material can be destroyed
2. The amount of material that can be destroyed in the least amount of time
3. The potential effect on national security should the material fall into hostile hands
4. The number of personnel required for destruction

5-70. When an emergency plan is implemented, which of the following material should be destroyed first?

1. SPECAT material
2. Special access material
3. COMSEC material
4. PERSONAL FOR material

5-71. In addition to having an emergency destruction plan, all commands are required to have what other type of emergency plan?

1. Fire
2. Evacuation
3. Security force
4. Watch security

5-72. Which of the following material should NOT be destroyed during a precautionary destruction?

1. Material of a historical nature
2. Material that has been superseded
3. Material essential to communications
4. Material that is unneeded

5-73. What should be done with superseded classified material?

1. Retain indefinitely
2. Retain for two years, then destroy
3. Retain for one month, then destroy
4. Destroy in accordance with its prescribed time frame